



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,218	04/19/2004	Wael M. Ibrahim	200314912-1	2929

22879 7590 01/29/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2436

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

01/29/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No. 10/827,218	Applicant(s) IBRAHIM ET AL.	
	Examiner MOHAMMAD W. REZA	Art Unit 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 October 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18, 45, 46, 48 and 49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18, 45-46, and 48-49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the arguments filed on 10/20/2008.
2. Claims 1-18, 45-46, and 48-49 are pending in the application.
3. Claims 1-18, 45-46, and 48-49 have been rejected.

Response to Amendment

4. The examiner approves the amendments made to claims 1, 2, 5-12, 18, 45.
5. The examiner approves addition of claims 48, and 49.
6. The examiner approves cancellation of claim 19-44, and 47.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-18, 45-46, and 48-49 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Applicant claims "migrating a non-migratable storage key". As the name emphasis "non-migratable storage key" means the key which should not be migrated or transferred. Any person ordinary skill in the art would normally understands and interprets from the name that the non-migratable key is non transferable. However, if someone wants to claim to transfer this key then there should be adequate support in

Art Unit: 2436

the specification how to make and use the claimed invention without undue experimentation. The examiner could not find anywhere in the specification that how to transfer this non-migratable storage key and where to transfer and thus the experimentation needed to practice the invention undue or Unreasonable. The analysis and conclusion of a lack of enablement are based on the factors discussed in MPEP § 2164.01(a) and 2164.04. In re Wands, 858 F.2d at 737, 8 USPQ2d at 1404 (Fed. Cir. 1988). See also United States v. Teletronics, Inc., 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988) (“The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation.”).

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-18, 45-46, and 48-49 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention “...**key storage hierarchy associated with a trusted platform module associated with the trusted platform;**” which is generally narrative and indefinite with the invention. Applicants do not point out clearly which options include in the present invention by this limitation. The normal understanding from the claim limitation to any ordinary skill in the art that the “**key storage hierarchy**” is associated with a trusted platform. Then, why it is again associated with the trusted platform. Examiner failed to

Art Unit: 2436

understand what is difference between these two trusted platforms from the claim. So this limitation is indefinite with the present application. The examiner will interpret these terms and limitations with the regarding claims as best understood for applying the appropriate art for rejection purposes. Appropriate correction needs to overcome the rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-18, 45-46, and 48-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener et al hereafter Weiss (US patent 6071190) in view of Cromer et al hereafter Cromer (US Patent 7,191,464).

10. As per claim 1, Challener discloses a system, comprising: a logic configured to perform cryptographic key maintenance where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform a trusted platform to which the logic is bound in a one-to-one manner and an interface configured to facilitate operably connecting the system to the trusted platform (abstract, paragraphs, 0007, 003-0031). He does not expressly disclose the logic is bound to in a

Art Unit: 2436

one-to-one manner with trusted platform. However, in the same field of endeavor, Cromer discloses the logic is bound to in a one-to-one manner with trusted platform (col. 4, lines 35-55, col. 3, lines 50-62).

Accordingly, it would be obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Cromer's teachings of bound the logic with one-to-one manner with the teachings of Chanllener, for the purpose of suitably using the non-migratable key to be migrated in the trusted platform.

11. As per claim 2, Challenger discloses the system where the cryptographic key maintenance performed by the logic comply with the Trusted Computing Group (TCG) specification version 1 .1b (paragraphs 0022-0024).

12. As per claim 3, Challenger discloses the system where the logic comprises an application specific integrated circuit (ASIC) (abstract, paragraphs, 0007, 003-0031).

13. As per claim 4, Challenger discloses the system where the logic comprises a microprocessor operably connected to a non-volatile memory (paragraphs, 0020).

14. As per claim 5, Challenger discloses a system where a logic configured to perform one or more of key maintenance, and cryptographic key migration and an interface configured to facilitate operably connecting the system to the trusted platform and where the logic and the interface comprise part of a USB token (abstract, paragraphs, 0007, 003-0031). He does not expressly disclose the logic is bound to in a one-to-one manner with trusted platform. However, in the same field of endeavor, Cromer discloses

Art Unit: 2436

the logic is bound to in a one-to-one manner with trusted platform (col. 4, lines 35-55, col. 3, lines 50-62).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

15. As per claim 6, Challenger discloses the system where the logic is configured to migrate one or more non-migratable keys from a trusted platform module associated with the trusted platform and configured to use the migrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module (abstract, paragraphs, 0007, 003-0031).

16. As per claim 7, Challenger discloses the system where the logic is Configured to perform performing cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform (paragraphs 0022-0024).

17. As per claim 8, Challenger discloses the system where the to perform performing cryptographic key maintenance includes including having the manufacturer of the trusted platform act as an intermediary and migrating [[a]] the non-migratable storage root key from [[a]] the root of [[a]] the key storage hierarchy associated with [[a]] the trusted platform module associated with the trusted platform (abstract, paragraphs, 0007, 003-0031).

18. As per claim 9, Challenger discloses the system where the logic is configured to performing cryptographic key migration including logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a

Art Unit: 2436

second protected storage tree (paragraphs, 0020).

19. As per claim 10, Challenger discloses the system where the logic is configured to store one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of [[a]] the trusted platform module, and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module (paragraphs 0022-0024).

20. As per claim 11, Challenger discloses the system where the logic is configured to facilitate substantially instantaneously restoring the trusted platform module (paragraphs, 0020).

21. As per claim 12, Challenger discloses the system where the logic is configured to decrypt one or more of, a key, and a piece of data encrypted by [[a]] the trusted platform module (paragraphs, 0020).

22. As per claim 13, Challenger discloses the system where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic (abstract, paragraphs, 0007, 003-0031).

23. As per claim 14, Challenger discloses the system where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic (paragraphs, 0020).

Art Unit: 2436

24. As per claim 15, Challenger discloses the system where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform (abstract, paragraphs, 0007, 003-0031).

25. As per claim 16, Challenger discloses the system where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic (paragraphs 0022-0024).

26. As per claim 17, Challenger discloses the system where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform (paragraphs, 0020).

27. As per claim 18, Challenger discloses the system the logic is configured to perform a finite number of cryptographic key maintenance operations (abstract, paragraphs, 0007, 003-0031).

28. As per claim 45, Challenger discloses a system, comprising: an electronic apparatus configured with a trusted platform module; and an interface operably connected to the electronic apparatus, and a subordinate trusted platform module to communicate with the trusted platform module via the interface, the subordinate trusted platform module including logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module (abstract, paragraphs, 0007, 003-0031). He does not expressly discloses the interface configured to facilitate operably, detachably connecting a subordinate trusted platform

Art Unit: 2436

module to the electronic apparatus. However, in the same field of endeavor, Cromer discloses the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus (col. 4, lines 35-55, col. 3, lines 50-62).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 45.

29. As per claim 46, Challenger discloses the system where the electronic apparatus comprises one of, a computer, a printer, a cellular telephone, and a digital camera (abstract, paragraphs, 0007, 003-0031).

30. As per claim 48, Challenger discloses the system where the interface includes a port, and the subordinate trusted platform module is embodied in a removable component that is attachable and detachable to the port (abstract, paragraphs, 0007, 003-0031).

31. As per claim 49, Challenger discloses the system where the subordinate trusted platform module is configured to use the migrated non-migratable storage root key to decrypt items that were encrypted by the trusted platform module (abstract, paragraphs, 0007, 003-0031).

Conclusion

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2436

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Art Unit: 2436

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser G Moazzami/

/Mohammad W Reza/

Supervisory Patent Examiner, Art Unit 2436

Examiner, Art Unit 2436